

**REMARKS**

Claims 1 - 43 are pending in the application and stand rejected. Claims 1, 14, 24, 28, 38 and 41 have been amended. Claims 12 - 13, 22 - 23, 29, 32 and 34 - 37 have been canceled. Claims 1 - 11, 14 - 21, 24 - 28, 30 - 31, 33 and 38 - 43 remain in the application and are presented for reconsideration.

Applicant's representative thanks the Examiner for the courtesy shown during a telephonic interview conducted on July 18, 2006. The substance of the interview was a discussion of the independent claims and the *Ballard* and *Randle, et al.* references. A draft amendment was faxed to the Examiner on July 11, 2006. Applicant's representative and the Examiner briefly discussed incorporating the limitation of a second biometric database of invalid users to determine if an individual presenting a transaction token is an authorized user of an account. However, no agreement was reached during the interview.

In the Office Action, the Examiner rejected claims 1 - 11, 14 - 21, 24 - 28, 30, 31 and 33 under 35 USC 35 USC §103(a) as being unpatentable over *Ballard* (U.S. 6,032,137) in view of *Randle, et al.* (U.S. 5,974,146). This rejection is respectfully traversed.

The Examiner must satisfy three criteria in order to establish a prima facie case of obviousness: (1) there must be some suggestion or motivation, either in the references themselves or in the knowledge of one of ordinary skill in the art, to modify the references or combine their teachings; (2) there must be a reasonable expectation of success; and (3) the prior art reference or combination of references must teach or suggest all the claim limitations. The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both

be found in the prior art and not based on applicant's disclosure. MPEP § 706.02(j), citing *In re Vaeck*, 20 USPQ 2d 1438 (Fed. Cir. 1991).

The amendments to independent claims 1, 14, 24, 28, 38 and 41 in this response are being made to further clarify and differentiate the present invention from the teachings of *Ballard* and *Randle, et al.* The Examiner did not provide appropriate rationale for the rejection of independent claims 38 and 41. This response is therefore treating these claims as having been rejected on the same basis as the other independent claims. The limitations recited in claims 12 – 13, 22 – 23, 29 and 32 have been added to claims 1, 14, and 28, respectively. These limitations include a second biometric database for invalid users (claims 12, 22, 29) and transmitting biometric data to the second biometric database to determine if an individual presenting a token is an invalid user (claims 13, 23, 32). The limitation recited in claims 34, 35, 36 and 37 of accepting or rejecting the transaction as the result from the comparisons with stored transaction information and biometric information has been added to claims 1, 14, 24 and 28, respectively. The other amendments to the independent claims will be discussed in the following remarks.

In the previous and current office actions, the Examiner has acknowledged that *Ballard* does not teach a real time electronic transaction verification system, and has combined the teachings of *Ballard* with another reference (either *Bezy et al.* or *Randle, et al.*) for teaching some aspect of a real time system in order to reject the pending claims.

The teachings of *Ballard* have been discussed at length in applicant's previous responses filed on May 11, 2005 and February 1, 2006. These responses are incorporated by reference to the extent they are not repeated below. *Ballard* teaches a remote image capture system with centralized processing and storage. The image capture system taught by *Ballard* batch processes

paper and/or electronic receipts such as credit card receipts, ATM receipts, business expense receipts, and sales receipts, and automatically generates reports such as credit card statements, bank statements, tax reports for tax return preparation, market analyses, etc. (col. 3, ll. 37 – 42, 59 – 64). It is an object of *Ballard's* system to *retrieve* both paper and electronic transactions at remote locations (col. 3, ll. 65 – 67).

The system taught by *Ballard* includes a remote data access subsystem (DATs 200) that scans documents including paper transaction data; a data collection subsystem (DACs 400) for collecting the completed transaction data from the DATs periodically; and a central data processing system (DPC 600) for processing and storing the completed transaction data. *Ballard* teaches polling and batch processing of data retrieved from the data access terminals. DPC 600 polls the DACs 400 to retrieve accumulated data received from the DATs. The DPC 600 stores the customer's data in a central location, generates reports from the data, and transmits the reports to credit card companies or transaction merchants at remote locations.

The entire process described in the flowchart of Fig. 3A involves batch processing of scanned paper receipts, i.e., the process occurs *after the transactions have been completed* and the paper receipts are available. Fig. 3B is an example of a paper receipt that is processed by a DAT. More specifically, it shows a paper receipt for a merchant that involves a separate credit card transaction. The Examiner has relied on the corresponding description of the credit card transaction discussed at col. 9, ll. 24 – 28 for a teaching of the reading device selectively transmitting transaction information to the transaction information database for comparison with account information stored for the authorized user. The credit card transaction is not part of the system taught by *Ballard*. Instead, it precedes the use of the DataTreasury system. The DAT

scans the information on the receipt and stores the information in a prescribed format that also includes the acquirer ID, the processor ID and the issuer ID.

The Examiner also cited *Ballard*, at col. 12, ll. 6 – 25, for gathering of real-time DAC server statistics for load balancing between DAC servers. Server load balancing is not part of the present invention. The sole purpose of server load balancing in real-time in *Ballard* is to direct the batch receipt data collected from DATs to DAC servers that are lightly loaded (col. 12, ll. 2 – 25). This does not constitute either an explicit or implicit teaching of a real time electronic transaction verification system.

The Examiner is relying on *Randle, et al.* for teaching of a real-time payment transaction system that will reject a transaction because of a bad card detection, or approve a transaction based on the consumer's PIN or biometric or other verification. *Randle, et al.* teaches an electronic commerce trust system (ECTS) as a real-time payment infrastructure (col. 1, ll. 42 – 43). The system taught by *Randle, et al.* requires that the retailer's customer be issued a "BITS" real-time debit card by a bank that is part of the ECTS network. The system can only be activated by use of the BITS card which contains an embedded chip. The card is verified through a "hot file" which contains an archive of lost, stolen or discontinued user cards and performs account verification, identification and authentication functions (col. 6, ll. 64 – 67). If the customer does not apply for and receive a BITS card, the retailer would be vulnerable to the presentment of fraudulent transactions tokens by those not enrolled in the system and would be unable to verify the condition of an account, the identity of the individual presenting the transaction token, and that the individual is the authorized user of the account. Another drawback of *Randle, et al.* is that it requires that the customer carry an extra card (i.e., the BITS debit card) in order to be

included in the payment system. Furthermore, since there is no biometric database taught by *Randle, et al.*, it would be easy for an identity thief to create a fraudulent BITS card having his own biometric on the fraudulent card. The thief's biometric at the point of sale would simply be compared with his own biometric on the fraudulent card. The hot file would not detect the fraudulent card since it only checks for lost, stolen or discontinued cards.

In contrast to *Randle, et al.*, the present invention does not require that the consumer carry any additional transaction cards or special transaction tokens. Customer enrollment in the system of the present invention can be accomplished at any time and at any member retailer that uses the system and methods of the present invention simply by the customer presenting a transaction token and registering a biometric such as a fingerprint at the transaction location. This differs from *Randle, et al.*, which requires that each customer apply for BITS membership and receive a bank-branded BITS card before the payment system can be used.

Furthermore, there is no teaching in either *Ballard* and *Randle, et al.* of returning a result from comparisons with both stored account information and stored biometric data for the authorized user to the transaction location to complete or reject a transaction in real time as recited in amended claims 1, 14, 24, 28, 38, and 41. Neither *Ballard* nor *Randle, et al.* teaches a *biometric databases* for storing biometric data for both an authorized user and an invalid user. The Examiner's citation to col. 11, l. 60 through col. 12, l. 5 in *Ballard* simply refers to the use of well known databases to store images and data received from DATs. This is not a teaching of biometric databases for storing biometric data for both authorized users and invalid users as recited in the independent claims.

Independent claims 1, 14, 24, 28, 38 and 41 include the limitations that the identity of the individual presenting the transaction token and the verification of a condition of a user account to complete the transaction are performed in real time with the result also being returned to the transaction location in order to accept or reject the transaction at the transaction location in real time. Conditions for rejecting the transaction could be, for example, and without limitation, "frequency of account access," "outstanding checks," "returned checks," and "account closed" as described in paragraph [015]. There is no teaching in *Ballard* of an electronic transaction verification system in which the condition of an authorized user's account is checked in real time as part of, and to complete, an electronic transaction. Furthermore, there is no teaching in *Ballard* of verifying that the individual presenting a transaction token to complete a transaction is an authorized user of an account stored in the system. Therefore, *Ballard* teaches away from a real time electronic transaction verification system as defined in the claims.

With respect to claims 1, 14, 24 and 28, *Ballard* fails to teach a transaction information database for storing account information for an authorized user. In *Ballard*, the customer is a vendor or a credit card merchant, not an authorized user of an account or individual presenting a transaction token at a transaction location. *Ballard* teaches the storing of receipts, not account information for an authorized user. The receipts that are electronically stored are picked up periodically (polled) by the DAC.

Furthermore, *Ballard* fails to teach an electronic transaction verification system for use at a location where a transaction token is presented, in which the reading device selectively transmits transaction information data to the information database for comparison with the account information stored for the authorized user to verify a condition of the account in real

time. Although *Ballard* teaches that the DAT could include devices for capturing biometric data for additional security, there is no teaching in *Ballard* or *Randle et al.* of a biometric data device selectively transmitting biometric data to a biometric database for comparison with biometric data stored for an authorized user to verify the identity of the individual presenting the transaction token in real time with the result of the comparison being returned to the transaction location in real time.

The Examiner stated that it would have been obvious to combine the teachings of *Ballard* and *Randle, et al.* However, modifying the *Ballard* system to enable real time electronic transaction verification would add a significant complexity, burden and overhead to the batch processing system. Neither *Ballard* nor *Randle, et al.* supports any required suggestion or motivation to make the proposed modification. All the claim limitations must be taught or suggested in the prior art. *Ballard* teaches a batch processing system for processing images of receipts captured at remote locations. *Randle, et al.* teaches a real-time bank-centric universal payment system requiring the use of a bank issued card with an embedded chip. The system of *Randle, et al.* is not activated until the chip card is activated by a PIN or biometric. Even if the teachings of *Ballard* and *Randle, et al.* could be combined, the complexity of the proposed modification suggests that a person skilled in the art would require significant inventive effort to combine the references as the Examiner suggests.

In view of the above arguments, claims 1, 14, 24, 28, 38 and 41 are allowable over the combination of *Ballard* and *Randle, et al.* Claims 2 – 11 depend from claim 1; claims 15 – 21 depend from claim 14; claims 25 – 27 depend from claim 24; claims 30 – 33 depend from claim 28; claims 39 – 40 depend from claim 38; and claims 42 – 43 depend from claim 41. Claims 2 –

11, 15 – 21, 25 – 27, 30 – 33, 39 – 40 and 42 - 43 also are allowable over the combination of *Ballard* and *Randle, et al.* for at least the same reasons that claims 1, 14, 24, 28, 38 and 41 are allowable over these references.

Claims 2, 15, 25 and 33 recite the limitation that the transmitted signature data is compared with the signature stored for the authorized user in the signature database in real time. *Ballard* teaches at col. 5, ll. 62 – 63, that DAT scanner 202 is capable of capturing handwritten signatures for identity verification. However, this is not a teaching of verifying the signature of an individual presenting a token in real time. *Randle et al.* does not teach capturing of an individual's signature at a transaction location for identification of the individual. Therefore, claims 2, 15, 25 and 33 are allowable over the combination of *Ballard* and *Randle, et al.* for this additional reason.

With respect to claims 6 and 18, *Ballard* teaches at col. 5, l. 52 – col. 6, l. 2, that DAT scanner 202 scans a paper receipt and generates a digital bitmap image representation of the receipt. The paper receipt captured by *Ballard* is not a teaching that transaction information data includes data encoded on the transaction token as recited in claims 6 and 18. Therefore, claims 6 and 18 are allowable over the combination of *Ballard* and *Randle, et al.* for this additional reason.

With respect to claims 7 and 19, *Ballard* teaches at col. 6, l. 58 – col. 7, l. 3, that the DAT card interface 212 can read transaction data from a smart card that has been lost, stolen, damaged, or deliberately altered in order to reproduce the transaction data for the customer (i.e., merchant). The DAT card interface 212 provides support for independent verification of records maintained by consumers, merchants, and bankers to prevent a loss of data. This is not a



teaching of selectively returning a report on customer usages by an electronic transaction verification system as recited in claims 7 and 19. Therefore, claims 7 and 19 are allowable over the combination of *Ballard* and *Randle, et al.* for this additional reason.

With respect to claims 8, 20, 26 and 31, *Ballard* teaches, at col. 6, ll. 53 – 58 and col. 7, ll. 41 – 44, that DATs 200 can include additional devices for capturing other biometric data for additional security. These devices include facial scans, fingerprints, voice prints, iris scans, retina scans, and hand geometry. *Ballard* further teaches that DAT controller 210 compresses, encrypts, and tags the bitmap image of a receipt to form a tagged encrypted compressed bitmap image. These teachings of *Ballard* do not constitute a teaching of selectively encoding recorded biometric data on the transaction token as recited in claims 8, 20, 26 and 31. In Applicant's invention, a transaction token is presented by an individual at the transaction location. It is not a paper or electronic receipt generated as a result of the completed transaction. Therefore, claims 8, 20, 26 and 31 are allowable over the combination of *Ballard* and *Randle, et al.* for this additional reason.

The Examiner rejected claims 12 – 13, 22 – 23, 29, 32, and 34 – 43 under 35 USC § 103(a) as being unpatentable over *Ballard*, in view of *Randle, et al.*, and further in view of *Hoffman, et al.* (U.S. Pat. No. 5,613,012). The Examiner applied the *Hoffman, et al.* teaching of a prior fraud database to claims 12 – 13, 22 – 23, 29 and 32. *Hoffman et al.* is directed to a tokenless identification system for authorization of electronic transactions and electronic transmissions. There is no teaching, suggestion or motivation in *Ballard, Randle, et al.* or *Hoffman et al.* to combine the fraud database for a tokenless electronic transaction system as taught by *Hoffman et al.* with the token-based transaction systems as taught by *Ballard* and

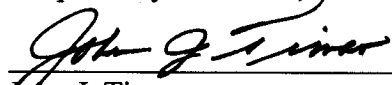
Serial No. 10/816,037  
Amendment Dated October 11, 2006  
In response to Office Action dated April 11, 2006

*Randle, et al.* Claims 12 – 13, 22 – 23, 29, 32 and 34 – 37 have been canceled with their limitations being added to claims 1, 14, 24 and 28. With respect to claims 38 – 43 this rejection is respectfully traversed. Claims 38 and 41 are independent claims that have been discussed above. Claims 39 – 40 and 42 – 43 depend from claims 38 and 41, respectively. Applicant incorporates by reference the arguments presented above for the allowability of claims 38 and 41 over the combined teachings of *Ballard* and *Randle, et al.* Applicant relies on the allowability of claim 38 for the allowability of claims 39 – 40. Applicant relies on the allowability of claim 41 for the allowability of claims 42 – 43.

In view of the above, it is submitted that the pending claims are in condition for allowance. Such action at an early date is earnestly solicited. It is also requested that the Examiner contact applicant's attorney at the telephone number listed below should this response not be deemed to place this application in condition for allowance.

10/11/06  
Date  
Womble Carlyle Sandridge & Rice, PLLC  
P.O. Box 7037  
Atlanta, GA 30357-0037  
(404) 888-7412 (Telephone)  
(404) 870-2405 (Facsimile)

Respectfully submitted,

  
\_\_\_\_\_  
John J. Timar  
Registration No. 32,497  
Attorney for Applicants